1) A DAC mechanism is used to control:

   a) the execution of programs.
   b) the modification of directories.
   c) the maximum size of files.
   d) All of the above.
   e) a) and b).
   f) b) and c).

2) Which classes allow the DAC protection on newly created objects todefault to public access?

   a) C1.
   b) C2.
   c) B1.
   d) a) and b).
   e) None of the above.

3) A user must possess access permission to an object before he can grantor revoke control permission to the object.

   a) TRUE.
   b) FALSE.

4) An ACL:

   a) provides finer granularity of DAC than permission bits.
   b) requires garbage collection when an object is deleted from the system.
   c) is associated with each subject to describe the access rights to that subject.
   d) is associated with each object to describe the access rights to thatobject.
   e) a) and c).
   f) b) and d)
   g) a) and d).

5) An application program outside of the operating system that carries out functions for a group of users, maintains some common data for all usersin the group, and protects the data from improper access by users in the groupis known as:

   a) a profile.
   b) a DAC ring.
   c) a wild card mechanism.
   d) a protected subsystem.
   e) a segment.

6) A capability list:

   a) maintains discretionary access rights for a subject.
   b) maintains an access control matrix.
   c) maintains discretionary access permissions for an object.
   d) cannot be used to implement DAC.
   e) None of the above.

The following information applies to questions 7 through 10.

A hierarchical “most specific” access control database identifiesgroup membership as:

(Group1: User1, User 2, User4)
(Group2: User2, User 3)
(Group3: User4)

Object Y’s ACL contains:

(User1, Read)
(User2, Write)
(Group1, Read, Write)
(Group3, Write)

7) Can User1 read object Y?

a) YES.
b) NO.

8) Can User2 read object Y?

a) YES.
b) NO.

9) Can User3 write object Y?

a) YES.
b) NO.

10) Can User4 write object Y?

a) YES.
b) NO.